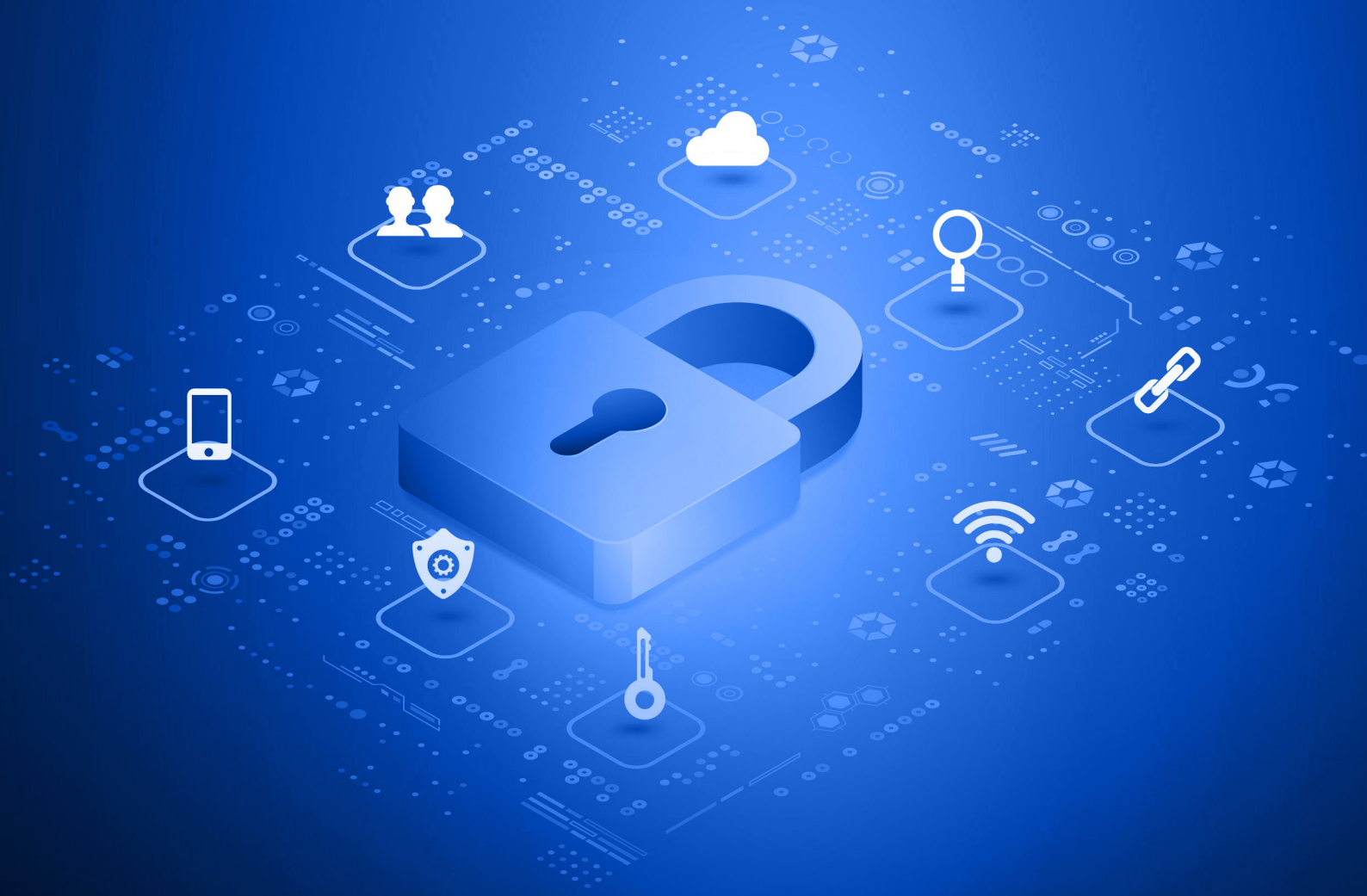
ignite

RECRUITMENT & TECHNOLOGY SOLUTIONS

Digital Health Checks The Value of Regular Cybersecurity Assessments



Introduction

As technology continues to transform the way we do business, cybersecurity has become more and more important. For small and medium enterprises (SMEs), the stakes are particularly high. A single cyber attack can not only bring operations to a halt but also erode customer trust and lead to significant financial losses. However, cybersecurity is a complex field, with an overwhelming number of approaches, solutions and standards available to organisations of all sizes.

In this context, how can organisations be confident they have the best possible cybersecurity coverage for their budget? How can they know they're getting a good return on their cybersecurity spending?

This is where regular cybersecurity assessments emerge as a critical tool for organisations to identify gaps in their defences, and opportunities to better safeguard their valuable data and networks.

A cybersecurity assessment is a comprehensive look at an organisation's information systems through a security lens. It involves a systematic evaluation of IT infrastructure, policies, and procedures, all with the goal of identifying vulnerabilities that could be exploited by cybercriminals. The assessment provides valuable insights and recommendations to fortify an organisation's defences, providing assurance and peace of mind.

On the following pages, we'll delve into several key benefits of regular cybersecurity assessments for Australian organisations, including compliance with regulations, financial savings, enhanced customer trust and how they ultimately contribute to an organisation's success in today's business landscape.

The Importance of Regular Cybersecurity Assessments

In the realm of cybersecurity, complacency is often the most costly mistake. Threats to cybersecurity are continuously evolving, with older attack methods becoming automated and sold 'as a service' to less skilled attackers, and newer techniques growing more sophisticated and potent. Modern cybercriminals use automated tools to scan the internet for targets that use specific software, exploiting weaknesses with little regard for the size of the organisation they're attacking.

A key aspect of a cybersecurity assessment is its systematic nature. Beginning with the identification of assets, followed by the assessment of threats and vulnerabilities, and culminates in an evaluation of the organisation's controls and defences. Findings are put in the context of the specific risks the organisation faces so that leaders can best decide how to prioritise their resources and efforts.

While one-time security assessments are certainly useful, they're usually not sufficient. This is because of the dynamic nature of cyber threats. What was secure yesterday may not be secure today. New vulnerabilities may have emerged, or existing defences may have been compromised. Maintaining a regular schedule of cybersecurity assessments can be the difference between business as usual and a potentially crippling cyber incident.

Regular cybersecurity assessments are particularly important for SMEs, which are often seen as 'soft targets' by cybercriminals—owing to their perceived lack of resources and cybersecurity expertise. Frequent assessments can help SMEs counter this perception, staying knowledgeable about the latest threats while ensuring they get the most out of a limited cybersecurity budget.

The Benefits of Regular Cybersecurity Assessments

Enhanced Security

The greatest and most obvious benefit of regular cybersecurity assessments is a stronger security posture. Cybersecurity assessments serve as a proactive way to identify and address vulnerabilities before they can be exploited by cybercriminals.

During an assessment, the organisation's entire IT infrastructure is evaluated—from hardware and software at all levels of the company to networks and data. The assessment scrutinises these components for vulnerabilities, including outdated software, weak passwords, unnecessary user privileges, and unprotected sensitive data.

In addition to identifying vulnerabilities, the assessment team will evaluate whether the organisation's existing security measures—from firewalls and intrusion detection systems to encryption protocols and more—are correctly configured, up to date, and effective against the current threat landscape.

When the assessment is complete, the organisation will receive a detailed report outlining all identified vulnerabilities, the effectiveness of existing security measures, and, most importantly, recommendations for improvement. These recommendations are tailored to the specific needs and context of the organisation, ensuring that they are both relevant and actionable.

Financial Savings

While it may be tempting to save money and only get a cybersecurity assessment when a problem has been identified, regular assessments usually help reduced costs for organisations in the long run. The cost of an assessment is an investment that can not only guide other cybersecurity spending but also help prevent potentially catastrophic losses from undiscovered vulnerabilities.

Cyberattacks can have a devastating financial impact on businesses. According to a report by the Australian Cyber Security Centre, the average cost of a cybercrime incident in Australia is $39,000 for a small business, $88,000 for a medium business, and over $62,000 for large businesses[1].

These costs can arise from several areas:

- **Operational downtime:** Cyberattacks can disrupt business operations, leading to a loss of productivity and revenue. The longer the disruption, the higher the costs.
- **Data recovery:** If a cyberattack results in data loss, the organisation may need to spend significant resources on data recovery or regeneration. Even worse, the data may be irretrievable, leading to permanent losses.
- **Legal costs and fines:** In addition to data recovery costs, organisations may face legal action from customers or partners affected by a data breach. They may also be fined for non-compliance with data protection regulations.

[1]https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

- **Reputational damage:** A cyberattack can be highly damaging to a business's reputation, not only because of disrupted services but also due to compromised customer data. More than 60% of respondents to a recent PwC survey expressed their willingness to switch service providers in the event of a cyber attack that disrupts their essential services. The figure jumps to 77% for Gen Z and Millennials.[2] Rebuilding a damaged reputation can be a long and costly process.

Regular cybersecurity assessments can help organisations avoid these costs. By identifying and addressing vulnerabilities, assessments can prevent cyberattacks from occurring in the first place. Even in cases where a cyberattack can't be entirely prevented, assessments help organisations put the best systems and procedures in place to respond to attacks effectively, minimising the impact and associated costs.

Improved Customer Trust

In the digital age, trust is one of an organisation's most valuable assets. Customers entrust organisations with their personal and financial information, and they expect this data to be protected.

When customers see that an organisation takes cybersecurity seriously—for example, by conducting regular assessments and responding to issues quickly—they're more likely to trust that organisation with their data. This trust can lead to increased loyalty, higher retention rates, and more business opportunities. This is double important to organisations in the business-to-business market, where one organisation's cybersecurity can impact the customer trust of another organisation.

Another way that cybersecurity assessments enhance customer trust is by helping organisations demonstrate their compliance with data protection regulations. Compliance with regulations such as the Australian Privacy Act 1988 and the General Data Protection Regulation (GDPR) in the European Union is often seen as a mark of trustworthiness, as it shows that the organisation is committed to protecting customer data.

For Australian SMEs, improved customer trust can be a significant competitive advantage. Smaller businesses tend to rely heavily on strong customer relationships, where trust is key. By conducting regular cybersecurity assessments, SMEs can strengthen this trust, leading to even stronger customer relationships and greater business success.

Risk Management

Risk management in all its forms can significantly impact an organisation's operations and profitability, and cybersecurity is no exception. As cyber threats become more automated and more frequent, cyber risk has become a critical aspect of overall risk management. Regular cybersecurity assessments are one of the most effective risk management tools an organisation can employ.

As with any type of risk management, the first step is understanding the risk landscape. Once risks are identified and assessed, the organisation can develop strategies to manage them. These include mitigating the risk (by implementing the recommendations from the assessment), transferring the risk (for example, through insurance), or accepting the risk (if the cost of mitigation exceeds the potential impact).

Regular cybersecurity assessments ensure that cyber risks are identified and assessed, and that any risk management strategies implemented remain effective over time. Again, as technology evolves, so does cyber risk. With regular assessments, an organisation can stay on top of the risks it faces and update its strategies accordingly.

Moreover, the insights from cybersecurity assessments can inform business decisions. For example, if an assessment identifies a significant vulnerability in a particular system, the organisation may decide to upgrade or replace that system. Similarly, if an assessment reveals that certain data is at high risk, the organisation may decide to limit the collection of or access to that data, or implement encryption measures.

[2]https://www.pwc.com.au/media/2021/pwc-community-attitudes-cyber-protect-essential-services.html

Conclusion

At first glance, conducting periodic cybersecurity assessments may seem like an unnecessary expense for small and medium businesses with a tight budget. The truth is, however, that with the constantly evolving nature of cyber crime and the high cost of a potential attack, cyber assessments are always a wise investment.

They provide a comprehensive, objective, and systematic assessment of an organisation's cybersecurity posture, helping the organisation stay ahead of potential threats and better target spending within limited budgets.

Regular cybersecurity assessments come with a wide variety of benefits. They enhance an organisation's security posture by identifying and addressing vulnerabilities. They ensure compliance with Australian and international regulations, helping organisations avoid legal complications and penalties. They lead to major financial savings by mitigating the high costs of cyberattacks. They foster customer trust, a key driver of business success. Last but not least, they provide valuable insights for risk management, leading to more informed decision-making and more efficient resource allocation.

For Australian SMEs, these benefits are particularly significant. In a digital marketplace where SMEs are often perceived as soft targets by cybercriminals, regular cybersecurity assessments can strengthen defences, build resilience, and enhance competitiveness.
Regular cybersecurity assessments are not just good practice; they're an essential tool for Australian SMEs aiming to thrive in the digital age.

Contact info

1300 481 179

www.igniteco.com

www.linkedin.com/company/igniteco

ignite
RECRUITMENT & TECHNOLOGY SOLUTIONS